The National Science Foundation
Office of Polar Programs
United States Antarctic Program

Information Resource Management Directive 5000.14
USAP Software Management and Protection

Organizational Function	Information Resource Management	Policy Number	5000.14
		Issue Date	1 August 2004
Policy Category	Information Security Policies and Procedures	Effective Date	1 August 2004
		Review On	1 August 2006
Subject	Software Management & Protection	Authorized By	Director, OPP
Office of Primary Responsibility	National Science Foundation Office of Polar Programs Polar Research Support Section	Responsible Official	Mr. Patrick D. Smith Technology Development Manager
Address	Suite 755 4201 Wilson Blvd Arlington, VA 22230	Phone	703.292.8032
		Fax	703.292.9080
		Web	www.nsf.gov/od/opp
Distribution	USAP-Wide	Status	Final Policy
Online Publication	www.polar.org/infosec/index.htm		

1. PURPOSE

This policy establishes the guidelines for the management and protection of software used within the National Science Foundation (NSF) Office of Polar Programs (OPP), United States Antarctic Program (USAP).

2. BACKGROUND

Software within information systems must be properly managed to ensure compliance with law and federal regulations regarding licensing and copyright infringement, and to protect against the effects of malicious applications.

3. GUIDING PRINCIPLES

- Proper licensing of software applications is essential to security of the USAP information infrastructure
- Current protective applications ensure the continuation of science and operations mission activities

4. POLICY

The USAP IT staff will manage all software used on USAP information systems to ensure appropriate licensing requirements are implemented. All USAP information systems will use some form of protection against malicious applications.

4.1 Operational Definitions

4.1.1 Malicious Application

Class of programs designed to cause some form of intentional damage, unauthorized access, or unexpected result to a system or network. Often referred to as "malware," and includes viruses, Trojan Horses, worms, and logic bombs. Attackers typically pass malware via email attachments, shared files, or removable media.

4.1.2 Virus

A program that is attached to an executable file or vulnerable application, and typically delivers an unwanted function that ranges from annoying to extremely destructive. A virus usually copies or sends its code to other programs or recipients. An executable email attachment that deletes other files when it is opened is an example of a virus. Viruses can also lay dormant and later be triggered by events such as date or keystrokes. The term "virus" is often ubiquitously used to describe any form of malicious application.

4.1.3 Trojan Horse

A Trojan Horse is an apparently useful, deliberately placed program or procedure, which contains hidden code that, when invoked, performs some unwanted function. Trojan horses may arrive hidden in software such as a game or graphics program.

4.1.4 Worm

A worm program has the primary goals of replication and propagation. A worm can typically make a copy of itself without needing to modify a host. A worm may (or may not) do things other than propagate. In the process of propagation, it may also have the effect of displacing storage space and bandwidth, which can slow down the affected systems. A worm program replicates itself and moves through shared network connections, emails, websites, removable media, unsecured ports, back doors (openings left by software vulnerabilities or malicious code), or other security holes, to infect other machines on the network. Viruses are often paired with a worm so that they can be spread faster and more broadly.

4.1.5 Logic Bomb

A program or setup which causes an endless loop cycle or other logic failure (like division by zero) thus hijacking system resources and/or eventually cause a failure. A complete computer "lockup" caused by opening an executable, which triggers an endless program loop is an example of a logic bomb. An email account that is set to auto-forwards it's mail to another email account that is already forwarding email to the first account is an example of a logic bomb "setup". The inbox on both email accounts will continue to expand until a failure occurs in one.

4.1.6 Spyware

An application that obtains information about a user, and reports that information to a collector for statistical analysis and other purposes. Spyware is often loaded without the user's awareness, and may sometimes be used to assist with an attack against the user, their systems, or their network.

4.2 General Policy Statements

The term "virus protection" is used synonymously to mean "malicious code protection" in this section.

4.2.1 Use of Malicious Code Protection Software

All USAP computers (desktops, laptops, personal digital assistants, etc.) connected to the USAP network must use the USAP approved virus protection software. Non-USAP computers connecting to the USAP network must meet vulnerability management requirements, including applicable anti-virus software requirements, before connecting to the USAP network.

4.2.2 Malicious Code Protection Software Status

All computers connecting to the USAP network infrastructure must have the latest version of virus protection software installed and enabled.

4.2.3 Malicious Code Protection Settings

The virus protection program settings must be configured for maximum effectiveness. In situations where this approach may interfere with the optimal performance of the affected system, the system owner will need to obtain a waiver from NSF OPP.

4.2.4 Malicious Code Protection Software Update Frequency

The update frequency of the virus protection software must be as soon as available from the vendor, and automatic where possible for all computers connecting to the USAP network. Systems that do not maintain current protection software will be removed from the network until their protection software is updated to the appropriate version.

4.2.5 File Servers

All USAP file servers must use USAP approved virus protection software, and be setup to detect and clean viruses that may infect files. Non-USAP file servers connecting to the USAP network must meet virus protection requirements before connection.

4.2.6 Email Gateways

Each USAP email gateway must use approved e-mail virus protection software and adhere to established rules for the setup and use of the software. Non-USAP email gateways connected to USAP networks must meet USAP system interface requirements, to include the need to address vulnerability management and virus protection.

4.2.7 Software Licenses

The USAP IT staff will ensure that all software used by USAP systems is properly licensed. Users and owners of non-USAP systems are responsible for ensuring their software is properly licensed. Any system using unlicensed software will be disconnected from the network until the licensing discrepancy is rectified.

4.2.8 Software License Records

The USAP prime contractor will ensure that all USAP software licenses are recorded by some mechanism, such as a central database, to be able to show proof of software license compliance. Non-USAP users, that have approved software, must be able to show proof of software compliance prior to connection to the USAP information infrastructure.

5. APPLICABILITY AND COMPLIANCE

This policy applies to all information resources, systems, and technology and to all users of these resources, systems and technology within the USAP operating environment or connected to the USAP information infrastructure. Compliance with this policy is as indicated in USAP Information Security Policy 5000.1, *The USAP Information Security Program*.

6. RESPONSIBILITIES

In addition to the responsibilities identified in USAP Information Resource Management Directive 5000.1, The USAP Information Security Program, the following officials have specific responsibilities related to Software Management and Protection.

6.1 USAP Information Security Manager (ISM)

The USAP ISM coordinates the implementation of the Software Management and Protection process across the USAP.

6.1 USAP Participant Organizations

Each USAP participant organization will establish a process and procedures to ensure all software is properly licensed and all appropriate steps are taken to manage know vulnerabilities and address antivirus requirements.

7. IMPLEMENTING SOFTWARE MANAGEMENT AND PROTECTION

7.1 Implementation

Each USAP participant organization will develop appropriate policies, processes, standards, and procedures to implement the USAP Information Security Software Management and Protection program. USAP participant organizations will publish procedures as appropriate to implement this program to comply with this policy. The USAP ISM will ensure that these procedures are uniformly administered across all sites. All users of the USAP infrastructure will ensure their systems comply with this policy.

7.2 Software Management and Protection - Program Administration.

The ISM will delegate, as necessary, administration of the Information Security Software Management and Protection program to competent personnel. Procedures for maintaining most current malicious code protection software installed and enabled on all USAP computers will be developed and made available to all users of USAP information resources. Procedures for ensuring software licensing compliance will be developed and made available to all users of USAP information resources.

7.3 Non-USAP Systems

Owners and operators of Non-USAP systems will ensure their systems use properly licensed software and implement appropriate measures to manage known vulnerabilities when their systems are connected to the USAP information infrastructure.

7.4 Policy Review

The USAP Information Security Program Manager will review this policy in conjunction with major changes to the information infrastructure, as part of the USAP's participation in agency security audits, after each breach in system security, or every two years. The ISM will submit policy changes and new policies for review and approval by NSF OPP

8. AUTHORITY

Publication of this policy is in conformance with the authority of the National Science Foundation Act of 1950, as amended and extended, the Federal Information Security Management Act of 2002 and NSF Manual 7, The NSF Information Security Handbook.

KARL A. ERB
Director